# Architecture

### Prérequis

un seul serveur où sera installé le serveur de la base de donnée et les applications web :

* Serveur de base de donnée Mysql 8
* Docker (plateforme de conteneurs)
* Nginx (reverse proxy)
* apps (sous forme de conteneur docker)
* iadmin (sous forme de conteneur docker)
* ibuy (sous forme de conteneur docker)
* sdm (sous forme de conteneur docker)
* ilogistics (sous forme de conteneur docker)
* qr (sous forme de conteneur docker)
* public (sous forme de conteneur docker)

### Spécifications du serveur

* Hardware
  + 48GO RAM minimum (6GO min pour chaque application pour un bon fonctionnement)
  + Une bonne Allocation CPU
  + 500GB minimum d’espace disque dur (pour accueillir le nombre important des ficher téléchargés depuis les applications)
* Software
  + Une installation fraîche de Ubuntu Server 20.04 (avec openssh-server)
    - <https://releases.ubuntu.com/focal/ubuntu-20.04.6-live-server-amd64.iso>
* Le serveur doit être connecté à internet (pour l’installation des applications et les prochaines MAJ des applications)

# **Installation**

### Installation de la base de donnée,docker et serveur nginx

Après l’installation Ubuntu Server 20.04 et la connexion avec le compte de l’utilisateur personnel, téléchargez et lancez le script d’installation a l’aide de ces commandes

cd ~

git clone https://github.com/azdadanass/orangeinit.git

cd orangeinit

chmod +x \*.sh

./install.sh

le script de l’installation install.sh contient les détails de l’installation sous forme de commentaires

Après l’installation il faut nécessairement redémarrer la machine

sudo reboot

### Installation de portainer

portainer est l’outil qui va permettre la gestion et la visualisation des logs des applications

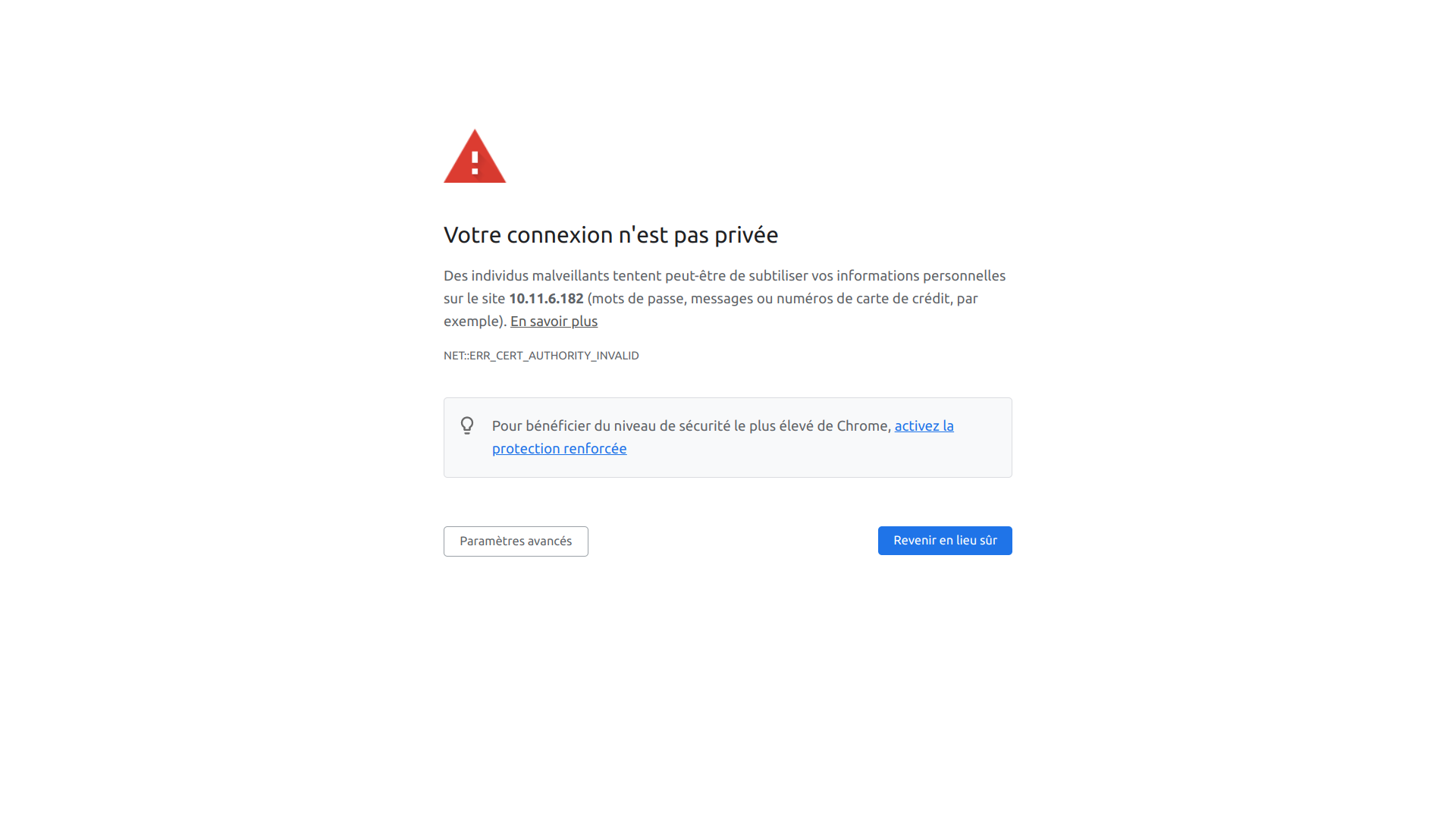
pour installer portainer, lancez le script suivant avec le compte de l’utilisateur personnel

~/orangeinit/deploy-portainer.sh

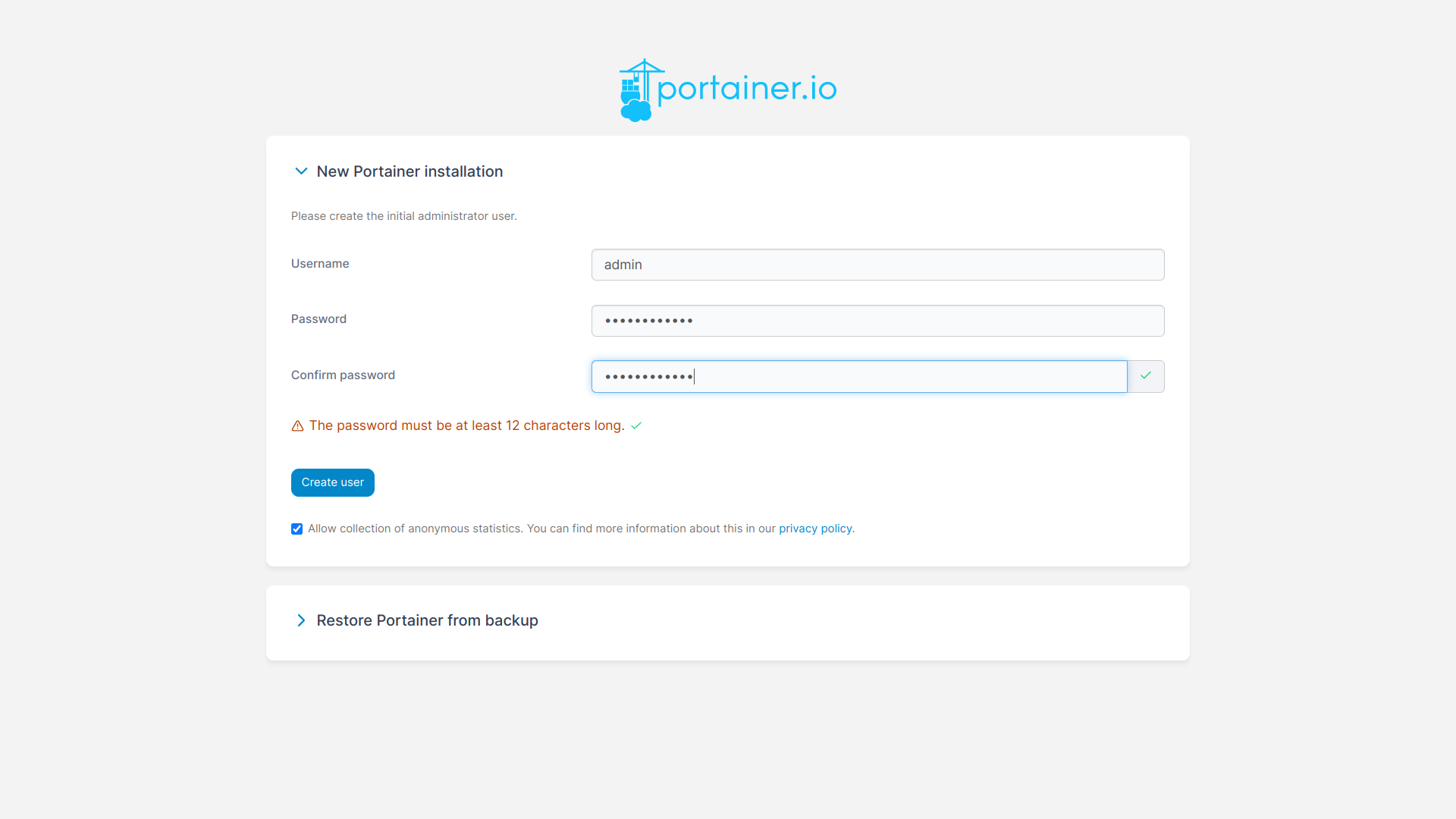
Après l exécution de la commande, vous pouvez accéder à l’interface depuis ce lien

https://ip\_de\_la\_machine:9443

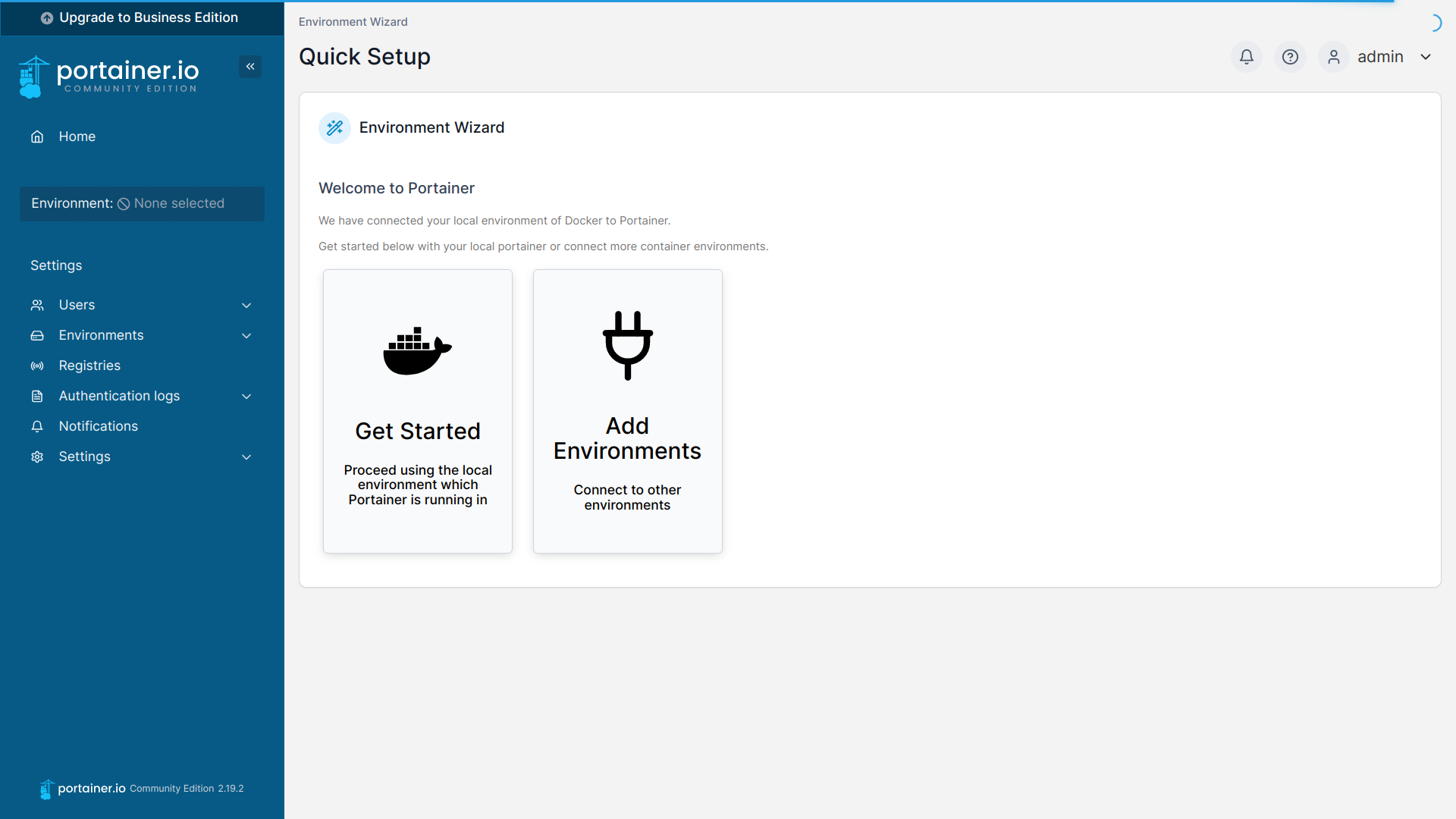
Cliquez sur Paramètres avancés, puis sur Continuer vers le site…



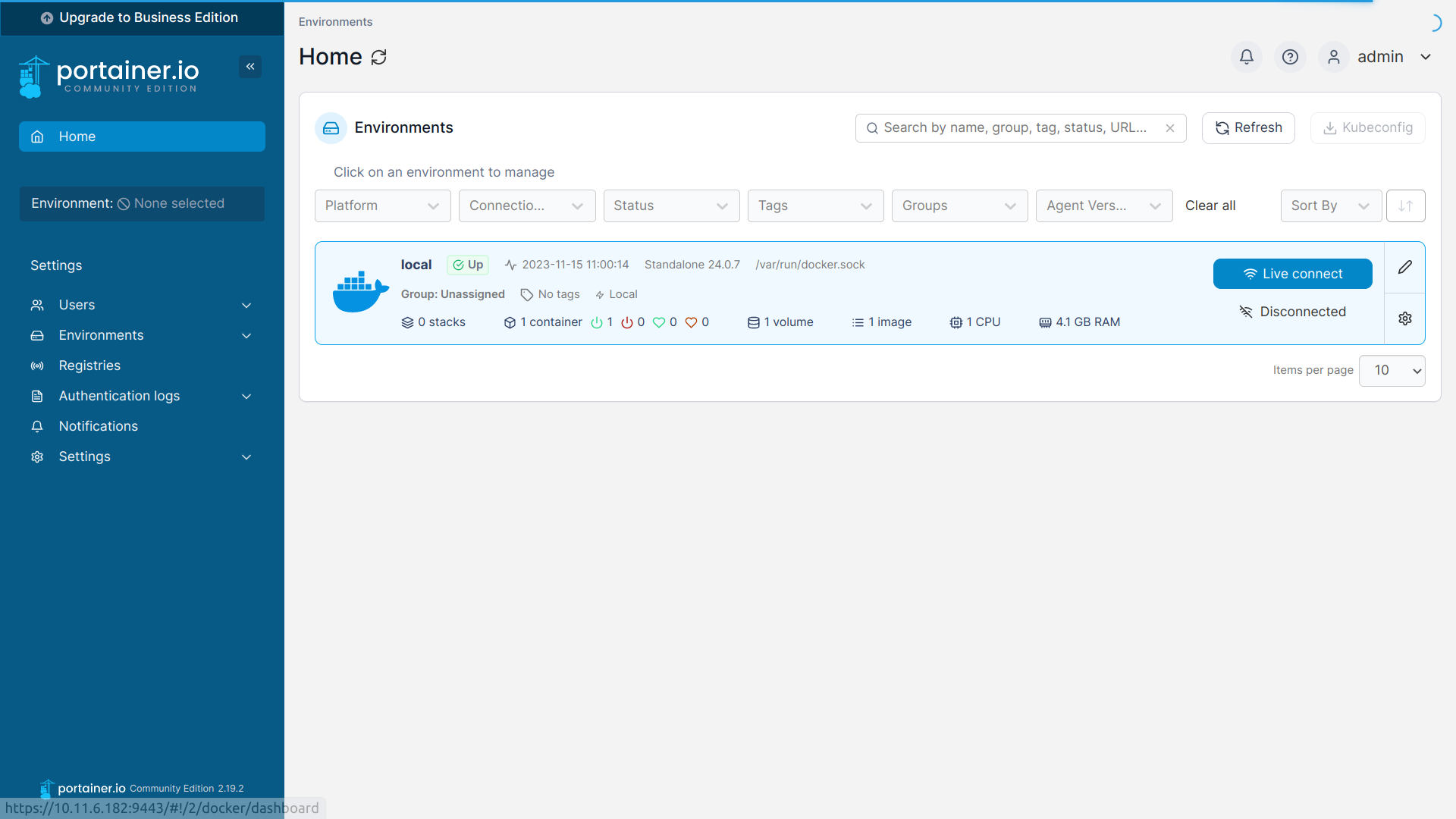
Le formulaire de création du compte admin vous sera proposé,créez le mot de passe admin puis cliquez sur create user



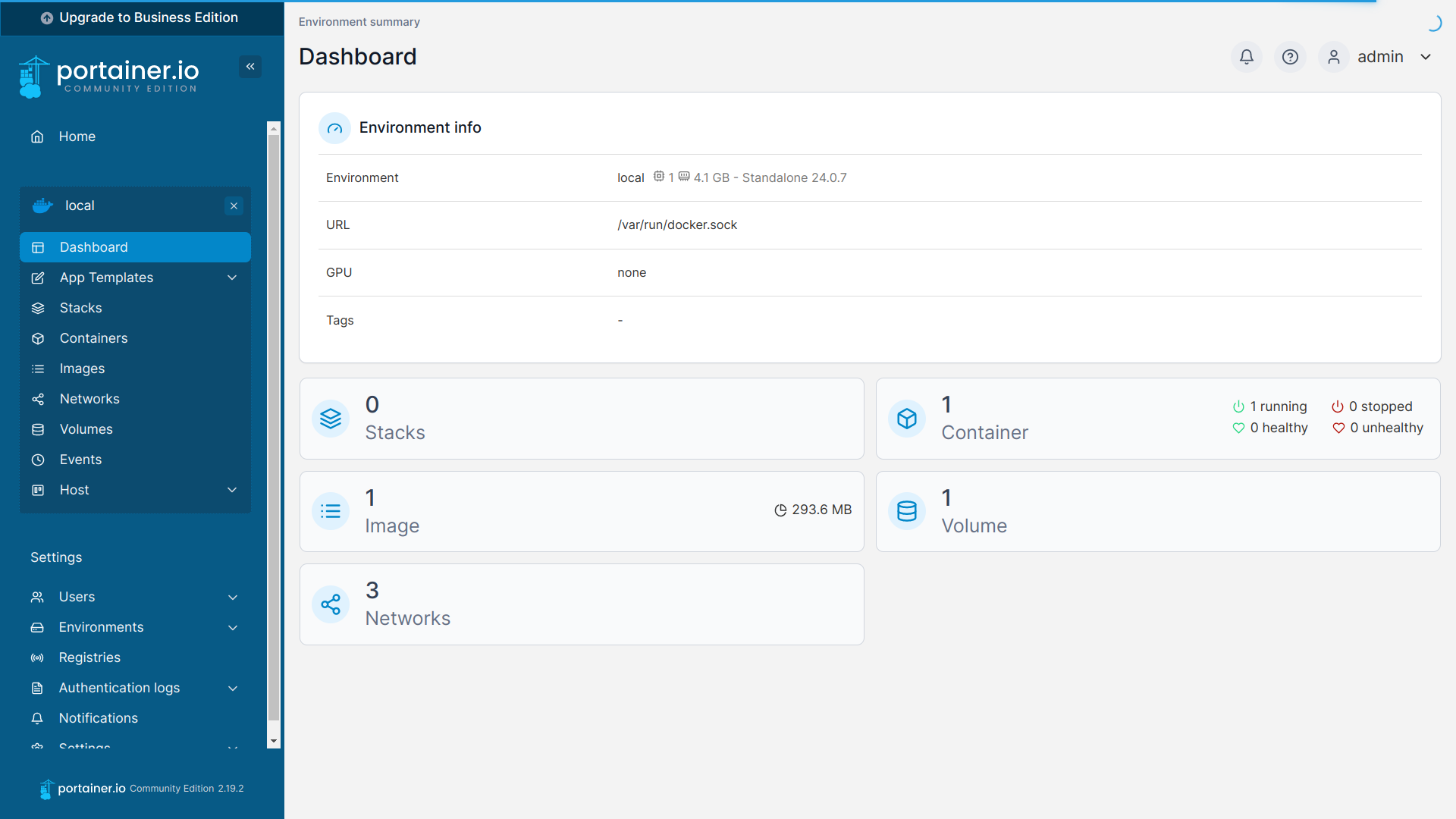
Dans le menu a gauche sélectionnez Home



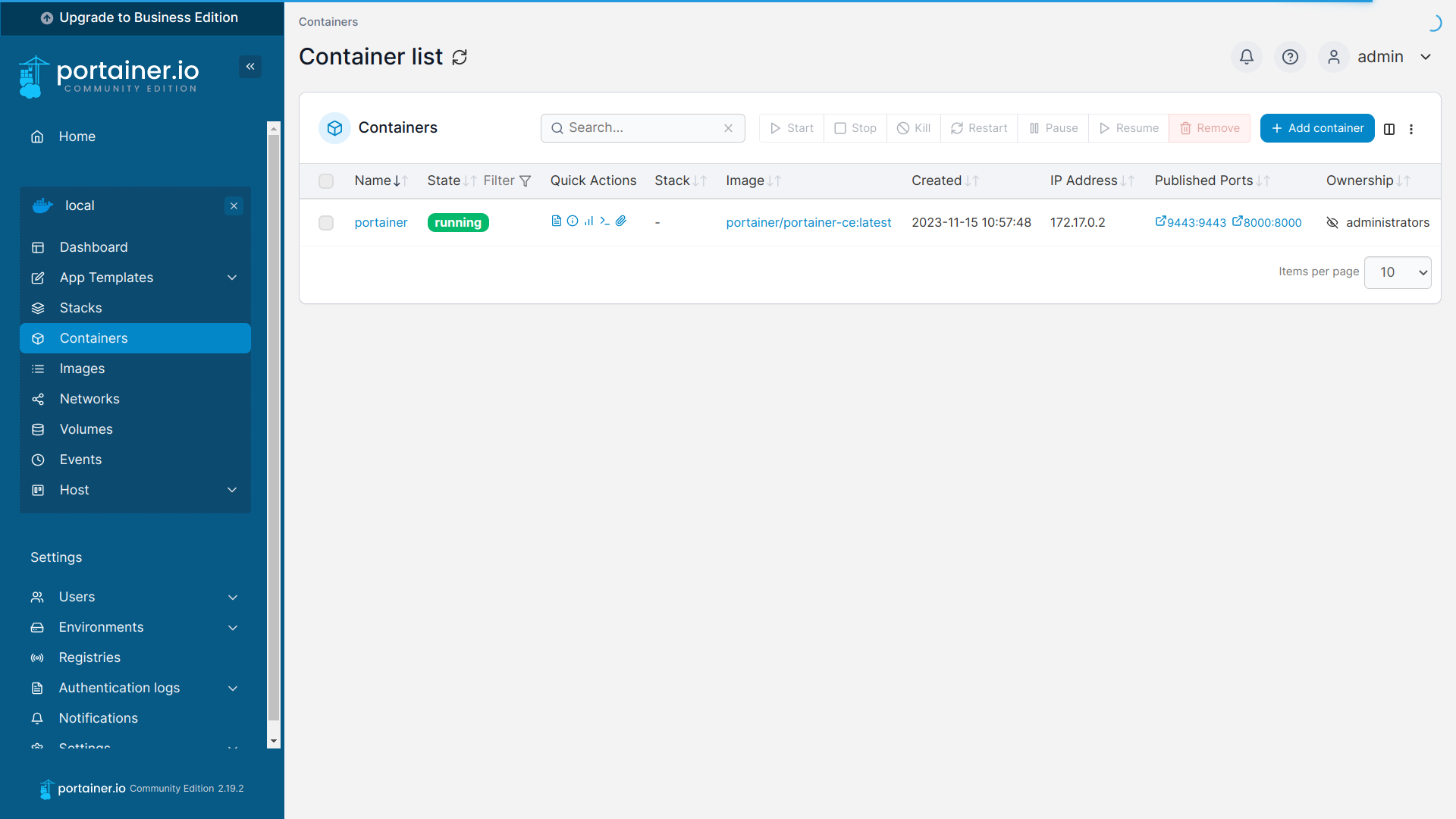
Cliquez sur l environnement local



Cliquer sur Container



Dans cette page, vous trouverez la liste des applications installées (pour l’instant seulement portainer est installé)



Mémorisez cette page, ça va nous permettre d’accéder aux logs des applications que nous allons installer par la suite

### Installation des applications (apps,iadmin ,sdm,ilogistics,public,qr,ibuy)

Pour installer ou faire la mise à jour des applications il suffit de lancer les commandes suivantes avec le compte de l’utilisateur personnel (chaque commande correspond a une application)

~/orangeinit/deploy-apps.sh

~/orangeinit/deploy-iadmin.sh

~/orangeinit/deploy-sdm.sh

~/orangeinit/deploy-ilogistics.sh

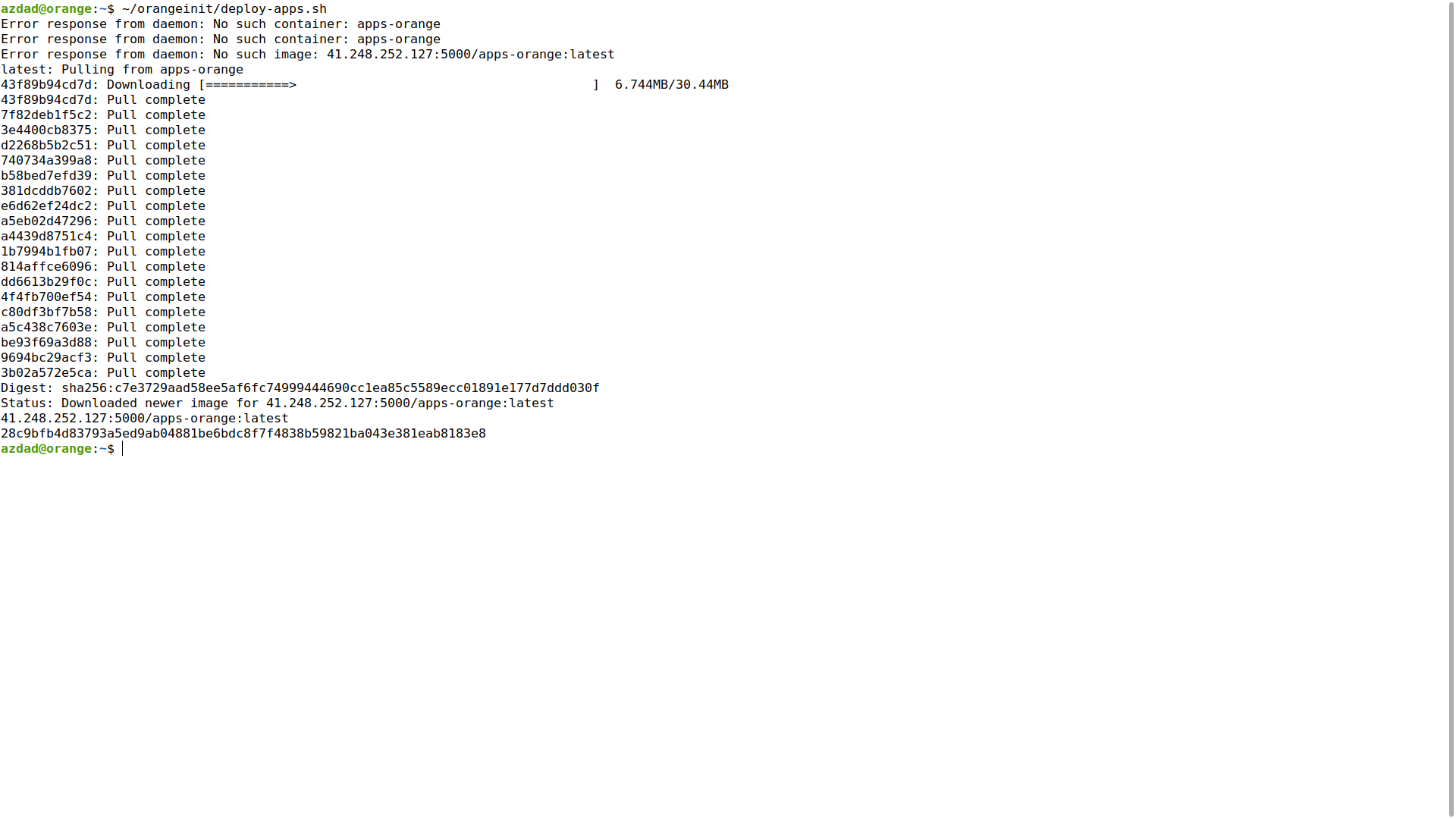
~/orangeinit/deploy-public.sh

~/orangeinit/deploy-qr.sh

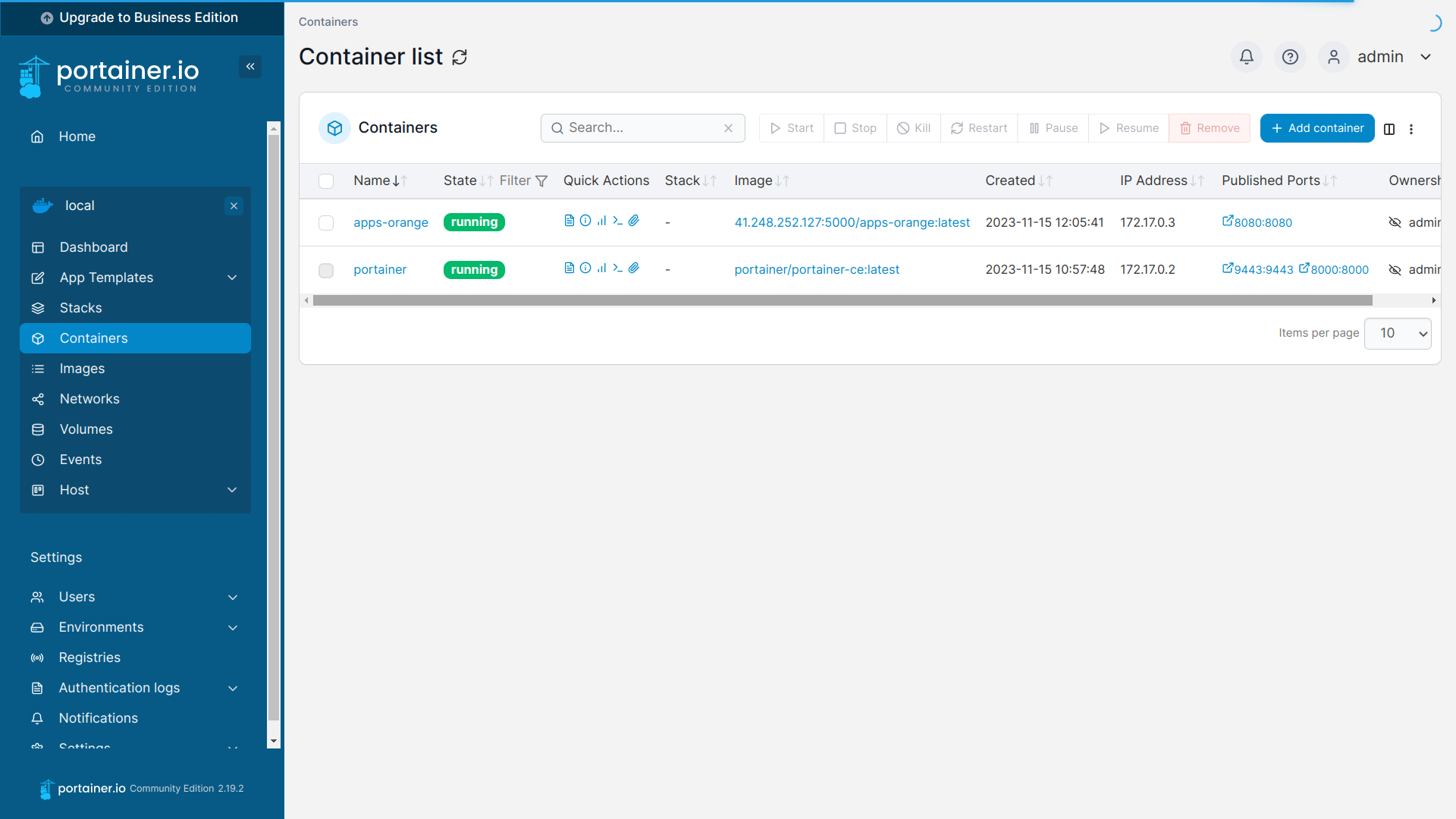
~/orangeinit/deploy-ibuy.sh

NB : pour la mise à jour d’une application , il faut coordonner avec le prestataire avant de lancer la commande de maj

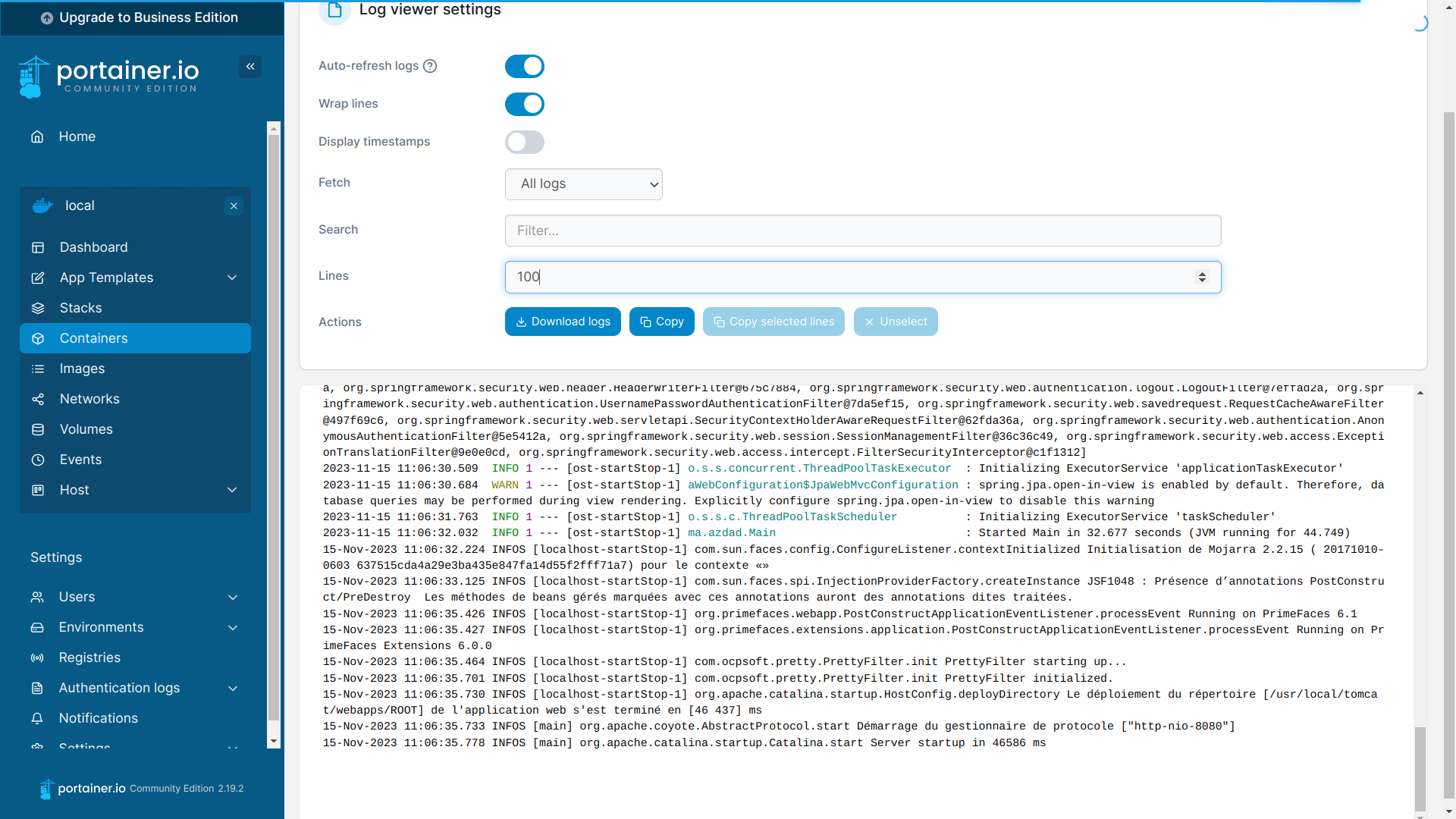
Exemple du lancement de apps



Après l’exécution de la commande ~/orangeinit/deploy-apps.sh,vous allez voir apparaître un nouveau container dans l’interface portainer

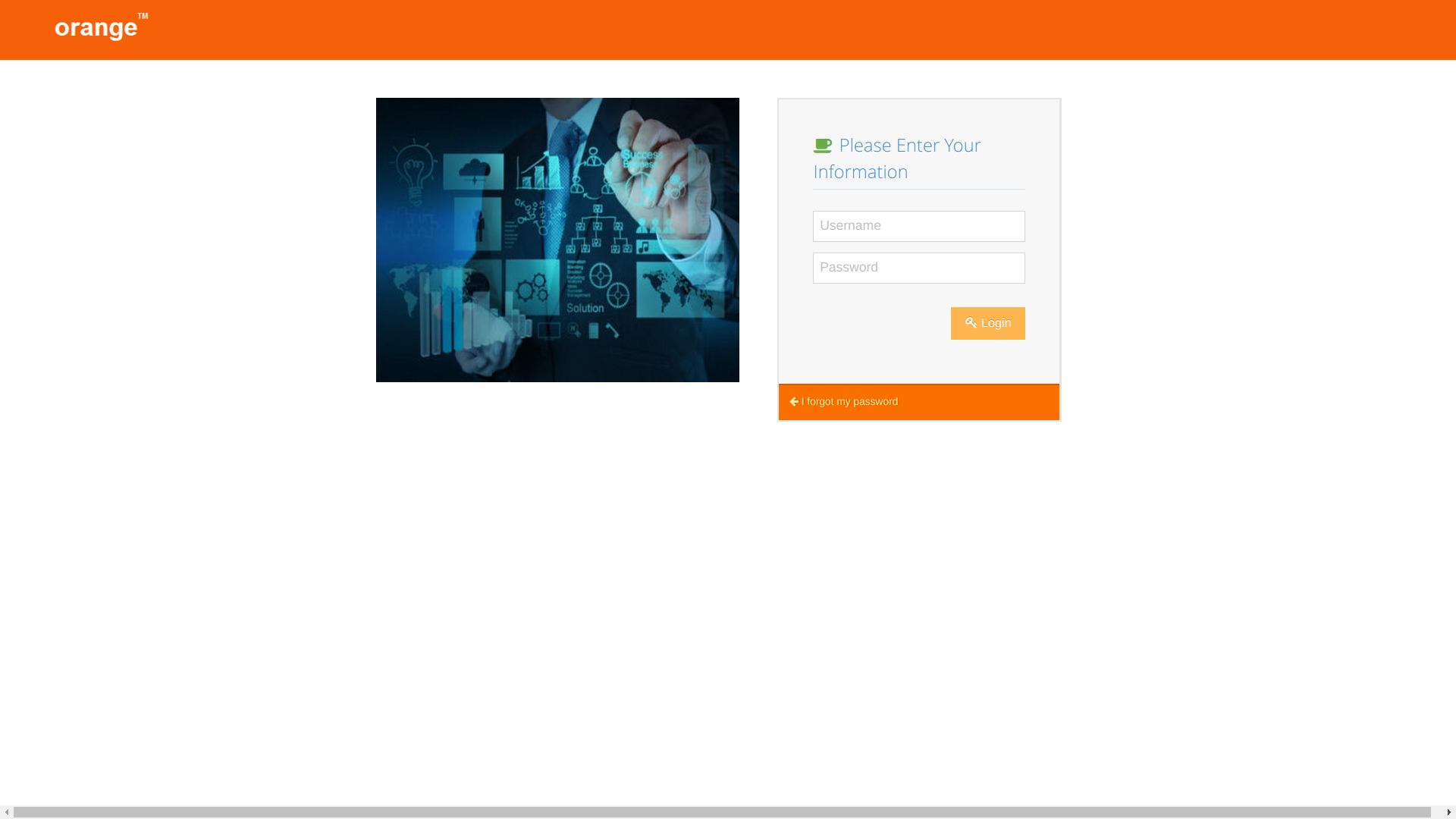


vous pouvez voir le log de apps-orange en cliquant sur l’icône de log dans Quick Actions, le log vous permettra de voir si le lancement de apps s’est bien déroulé



Si tout s’est bien déroulé,vous pouvez tester l’application apps-orange depuis ce lien :

http://ip\_de\_la\_machine:8080



pour les autres applications :

|  |  |
| --- | --- |
| Apps | [http://ip\_de\_la\_machine:8080](http://ip_de_la_machine:8080/) |
| iadmin | [http://ip\_de\_la\_machine:808](http://ip_de_la_machine:8080/)1 |
| sdm | [http://ip\_de\_la\_machine:808](http://ip_de_la_machine:8080/)2 |
| ilogistics | [http://ip\_de\_la\_machine:808](http://ip_de_la_machine:8080/)3 |
| public | [http://ip\_de\_la\_machine:808](http://ip_de_la_machine:8080/)4 |
| qr | [http://ip\_de\_la\_machine:808](http://ip_de_la_machine:8080/)5 |
| ibuy | [http://ip\_de\_la\_machine:808](http://ip_de_la_machine:8080/)6 |

NB : ces liens seront utilisés dans la configuration du reverse proxy nginx. Dans la partie qui viendra après, les ports [8080-8086] seront désactivés pour forcer seulement l’accès https (443)

1. **Configuration pour accès HTTPS**
2. Pour le moment, nos applications sont accessibles depuis les port [8080-8086] en http
3. pour passer en https, vous devez suivre ces étapes
4. Prenons l’exemple de iadmin (supposons que le nom de domaine qui a été attribué à iadmin par l’équipe de DNS est iadmin.example.com )
5. Nous devons commencer par créer le CSR
6. sudo mkdir -p /etc/nginx/ssl/
7. sudo openssl req -new -newkey rsa:2048 -nodes -keyout /etc/nginx/ssl/iadmin.key -out /etc/nginx/ssl/iadmin.csr
8. Vous devez remplir le formulaire comme suit (Common Name étant le champs le plus important, vous devez entrez le nom de domaine de iadmin fourni par l’équipe DNS, dans notre exemple c’est iadmin.example.com)
9. Country Name : MA
10. State : Casablanca
11. Locality Name : Casablanca
12. company : orange
13. Organizational Unit Name : delivery
14. Common Name : iadmin.example.com
15. Email address : vous pouvez laisser ce champs vide
16. A challenge password : vous pouvez laisser ce champs vide
17. An optional company name : vous pouvez laisser ce champs vide
18. Deux fichiers seront générés dans le dossier /etc/nginx/ssl ,qui sont iadmin.key et iadmin.csr
19. Vous devez fournir le fichier iadmin.csr à l’équipe responsable de la génération des certificat https qui vont générer le certificat (iadmin.crt)
20. Il suffit maintenant de placer le fichier crt reçu dans /etc/nginx/ssl/iadmin.crt (la nomination du fichier est importante)
21. Vous devez faire cette action pour les autres applications :

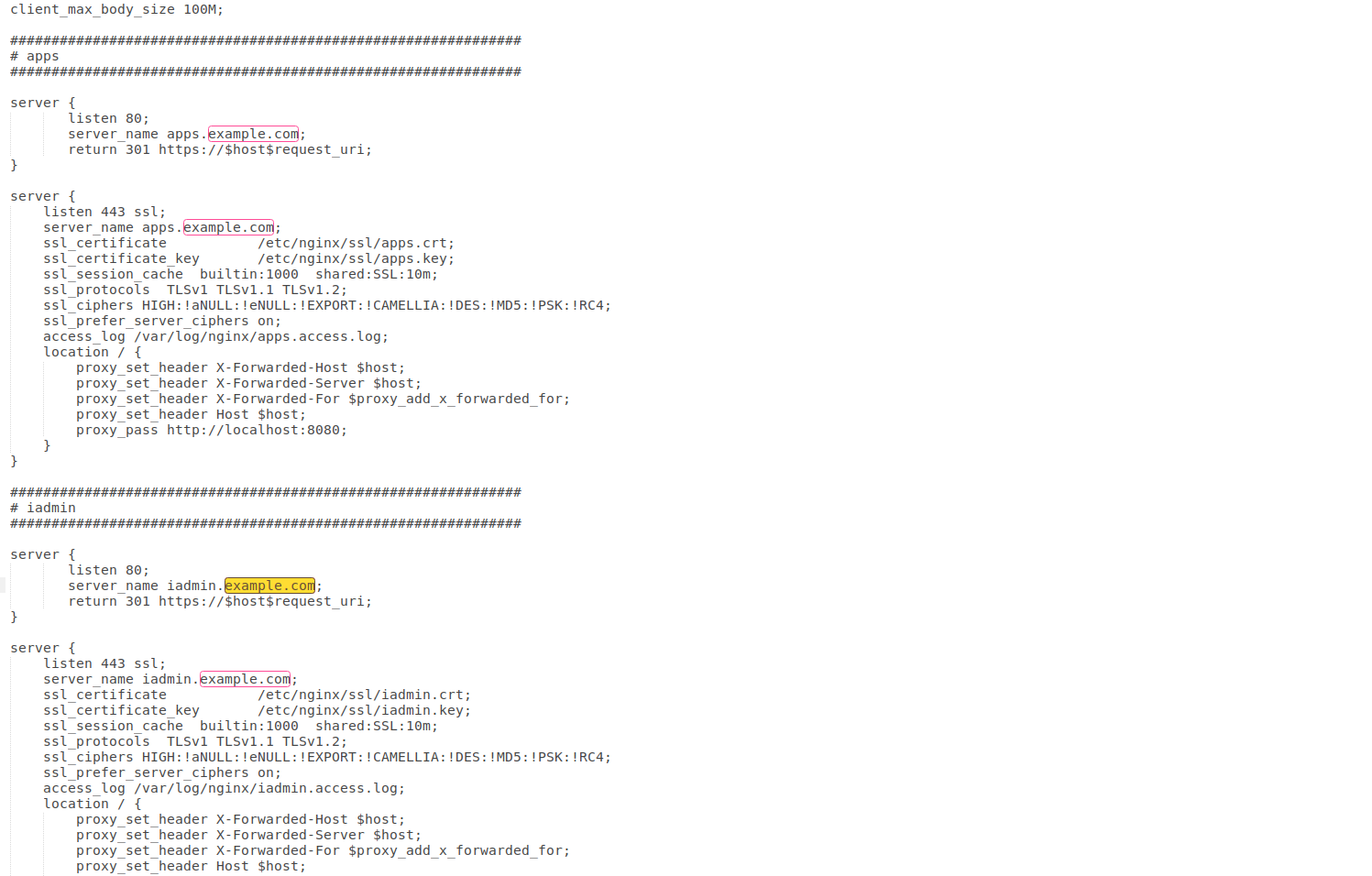
* apps
* sdm
* ilogistics
* qr
* public
* ibuy

### Configuration du reverse proxy nginx

Pour configurer le reverse proxy il suffit de lancer la commande

sudo nano /etc/nginx/sites-enabled/default

puis corriger le domaine example.com par le domaine fourni par l’équipe responsable des DNS



Après la sauvegarde du fichier (Ctr x + Yes), vous devez redémarrer nginx avec cette commande :

sudo service nginx restart

Après l’exécution de cette dernière commande, les applications devront être accessibles depuis les liens corrects en mode https

https://apps.example.com

https://iadmin.example.com

https://sdm.example.com

https://ilogistics.example.com

https://public.example.com

https://qr.example.com

https://ibuy.example.com

### **Activation et configuration du par-feu**

Pour configurer le par-feu, il suffit de lancer la commande suivante

~/orangeinit/ufw.sh

Après l’exécution de cette dernière commande, seuls les ports 80 (http) et 443 (https) seront accessible

**Backup et restauration**

Seuls la base de donnée et le dossier ~/files qui doivent être sauvegardés

Pour le dossier ~/files il suffit de faire une copie dans un serveur distant (serveur de backup) avec un outil tel que rsync

exemple

rsync -azv ~/files/\* user@ip\_server\_backup:/home/user/backup/files

Pour la base de donnée, Utilisez l’outil mysqldump pour avoir un fichier sql de la base de donnée et le copier dans le serveur distant

exemple

mysqldump \

--defaults-extra-file=/scripts/config.cnf \

--max\_allowed\_packet=1G --default-character-set=utf8 \

--single-transaction=TRUE "orange" \

--databases > ~/export/orange\_backup\_20231201.sql

rsync -azv ~/export/orange\_backup\_20231201.sql [user@ip\_server\_backup](mailto:user@ip_server_backup):/home/user/backup/db

Vous pouvez mettre les scripts des backups dans crontab et définir la fréquence des backups